**IN THE UNITED STATES DISTRICT COURT**
**FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

| | |
|---|---|
| IN THE MATTER OF THE SEARCH OF ROOM 17 AT THE PENN AMISH MOTEL, 2840 NORTH READING ROAD, DENVER, PENNSYLVANIA, 17517 | Case No. 21-mj-188<br><br>**Filed Under Seal** |

**AFFIDAVIT IN SUPPORT OF**
**AN APPLICATION FOR A SEARCH WARRANT**

I, Eric R. Patterson, being first duly sworn, hereby depose and state as follows:

## INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with Federal Bureau of Investigation (FBI) and have been so since January 2006. I have investigated federal criminal violations of the United States Code related to criminal matters and national security matters; specifically, related to international terrorism and domestic terrorism. I am currently assigned to the national security squad in the FBI Philadelphia Division, Harrisburg Resident Agency, Joint Terrorism Task Force, with a primary duty of investigating domestic terrorism matters. As a federal agent, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer, I am authorized to execute warrants issued under the authority of the United States.

2. On or about January 25, 2021, the Honorable Zia M. Faruqui, United States Magistrate Judge for the District of D.C., issued an arrest warrant (the "Arrest Warrant") for Zachary Alam, after finding probable cause to believe that Alam had violated the following statutes (the "Subject Offenses") when he participated in January 6, 2021, events at the United States Capitol:

a. 18 U.S.C. §§ 111(a) and (b), which make it a crime to forcibly assault, resist, oppose, impede, intimidate, or interfere with any person designated in [18 U.S.C. § 1114] while engaged in or on account of the performance of official duties; and punish the commission of such acts using a deadly or dangerous weapon. Pursuant to 18 U.S.C. § 1114, officers of the U.S. Capitol Police are "officers and employees of the United States or of any agency in any branch of the United States government."
b. 18 U.S.C. § 231(a)(3), which makes it unlawful to commit or attempt to commit any act to obstruct, impede, or interfere with any fireman or law enforcement officer lawfully engaged in the lawful performance of his official duties incident to and during the commission of a civil disorder which in any way or degree obstructs, delays, or adversely affects commerce or the movement of any article or commodity in commerce

or the conduct or performance of any federally protected function. For purposes of Section 231 of Title 18, a federally protected function means any function, operation, or action carried out, under the laws of the United States, by any department, agency, or instrumentality of the United States or by an officer or employee thereof. This includes the Joint Session of Congress where the Senate and House count Electoral College votes.

c. 18 U.S.C. § 1361, which makes it a crime to willfully injure or depredate any property of the United States.
d. 18 U.S.C. § 1512(c)(2), which makes it a crime to obstruct, influence, or impede any official proceeding, or attempt to do so. Under 18 U.S.C. § 1515, congressional proceedings are official proceedings.
e. 18 U.S.C. §§ 1752(a) and (b). Section 1752(a) makes it a crime to (1) knowingly enter or remain in any restricted building or grounds without lawful authority to do so, (2) knowingly, and with intent to impede or disrupt the orderly conduct of Government business or official functions, engage in disorderly or disruptive conduct in, or within such proximity to, any restricted building or grounds when, or so that, such conduct, in fact, impedes or disrupts the orderly conduct of Government business or official functions, or (4) knowingly engage in any act of physical violence against any person or property in any restricted building or grounds, or attempt or conspire to do so; and § 1752(b) punishes the commission of such acts if the person, during and in relation to the offense, uses or carries a deadly or dangerous weapon. For purposes of Section 1752 of Title 18, a "restricted building" includes a posted, cordoned off, or otherwise restricted area of a building or grounds where the President or other person protected by the Secret Service, including the Vice President, is or will be temporarily visiting; or any building or grounds so restricted in conjunction with an event designated as a special event of national significance.
f. 40 U.S.C. §§ 5104(e)(2)(D), (F) and (G), which make it a crime to willfully and knowingly (D) utter loud, threatening, or abusive language, or engage in disorderly or disruptive conduct, at any place in the Grounds or in any of the Capitol Buildings with the intent to impede, disrupt, or disturb the orderly conduct of a session of Congress or either House of Congress, or the orderly conduct in that building of a hearing before, or any deliberations of, a committee of Congress or either House of Congress; (F) engage in an act of physical violence in the Grounds or any of the Capitol Buildings; and (G) parade, demonstrate, or picket in any of the Capitol Buildings.

3. On or about the morning of January 30, 2021, FBI agents arrested Alam in Room 17 of the Penn Amish Motel, located at 2840 North Reading Road in Denver, Pennsylvania (the "Subject Premises," which is further described in Attachment A). This affidavit is made in support of an application for a search warrant for the Subject

Premises. As described below, there is probable cause to believe that the Subject Premises contain evidence, fruits, and/or instrumentalities of the Subject Offenses.

4. I base the facts set forth in this affidavit upon my personal knowledge, information obtained during my participation in this investigation, review of documents to include cellphone records, knowledge obtained from other individuals including law enforcement personnel, and communications with others who have personal knowledge of the events and circumstances described herein. Because this affidavit is being submitted for the limited purpose of enabling this Court to make a judicial determination of probable cause to issue a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish the legal basis for the issuance of a search warrant.

## PROBABLE CAUSE

### *Background – The U.S. Capitol on January 6, 2021*

6. The United States Capitol Police ("USCP"), the FBI, and assisting law enforcement agencies are investigating a riot and related offenses that occurred at the United States Capitol Building, located at 1 First Street, NW, Washington, D.C., 20510 at latitude 38.88997 and longitude -77.00906 on January 6, 2021.

7. At the U.S. Capitol, the building itself has 540 rooms covering 175,170 square feet of ground, roughly four acres. The building is 751 feet long (roughly 228 meters) from north to south and 350 feet wide (106 meters) at its widest point. The U.S. Capitol Visitor Center is 580,000 square feet and is located underground on the east side of the Capitol. On the west side of the Capitol building is the West Front, which includes the inaugural stage scaffolding, a variety of open concrete spaces, a fountain surrounded by a walkway, two broad staircases, and multiple terraces at each floor. On the East Front are three staircases, porticos on both the House and Senate side, and two large skylights into the Visitor's Center surrounded by a concrete parkway. All of this area was barricaded and off limits to the public on January 6, 2021.

8. The U.S. Capitol is secured 24 hours a day by USCP. Restrictions around the U.S. Capitol include permanent and temporary security barriers and posts manned by USCP. Only authorized people with appropriate identification are allowed access inside the U.S. Capitol.

9. On January 6, 2021, a joint session of the United States Congress was scheduled to convene at the U.S. Capitol to certify the vote count of the Electoral College of the 2020 Presidential Election, which took place on November 3, 2020 ("Certification"). The exterior plaza of the U.S. Capitol was closed to members of the public.

10. A crowd began to assemble near the Capitol around 12:30 p.m. Eastern Standard Time (EST), and at about 12:50 p.m., known and unknown individuals broke

through the police lines, toppled the outside barricades protecting the U.S. Capitol, and pushed past USCP and supporting law enforcement officers there to protect the U.S. Capitol.

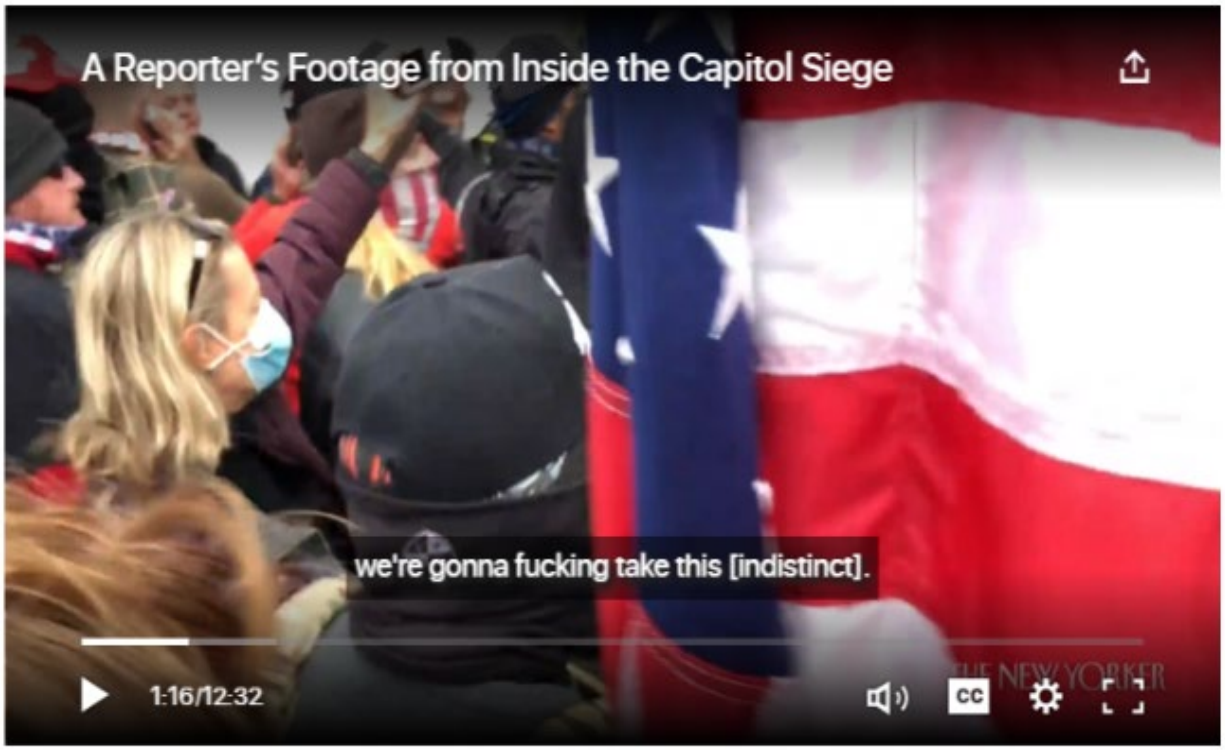
11. The joint session began at approximately 1:00 p.m. in the House Chamber.

12. At approximately 1:30 p.m., the House and Senate adjourned to separate chambers to resolve a particular objection. Vice President Mike Pence was present and presiding, first in the joint session, and then in the Senate chamber. Also around this time, USCP ordered Congressional staff to evacuate the House Cannon Office Building and the Library of Congress James Madison Memorial Building, in part because of a suspicious package found nearby. Pipe bombs were later found near both the Democratic National Committee and Republican National Committee headquarters.

13. As the proceedings continued in both the House and the Senate, USCP attempted to keep the crowd away from the Capitol building and the proceedings underway inside. Media reporting showed a group of individuals outside of the Capitol chanting, "Hang Mike Pence." I know from this investigation that some individuals believed that Vice President Pence possessed the ability to prevent the certification of the presidential election and that his failure to do so made him a traitor.

14. At approximately 2:00 p.m., some people in the crowd forced their way through, up, and over additional barricades and law enforcement. The crowd advanced to the exterior façade of the building. The crowd was not lawfully authorized to enter or remain in the building and, prior to entering the building, no members of the crowd submitted to security screenings or weapons checks by USCP officers or other authorized security officials. At such time, the certification proceedings were still underway and the exterior doors and windows of the U.S. Capitol were locked or otherwise secured. Members of law enforcement attempted to maintain order and keep the crowd from entering the Capitol.

15. At about 2:10 p.m., individuals in the crowd forced entry into the U.S. Capitol, including by breaking windows and by assaulting members of law enforcement, as others in the crowd encouraged and assisted those acts. Publicly available video footage shows an unknown individual saying to a crowd outside the Capitol building, "We're gonna fucking take this," which your affiant believes was a reference to "taking" the U.S. Capitol.




16. Shortly thereafter, at approximately 2:20 p.m. members of the United States House of Representatives and United States Senate, including the President of the Senate, Vice President Mike Pence, were instructed to—and did—evacuate the chambers. That is, at or about this time, USCP ordered all nearby staff, Senators, and reporters into the Senate chamber and locked it down. USCP ordered a similar lockdown in the House chamber. As rioters attempted to break into the House chamber, by breaking the windows on the chamber door, law enforcement were forced to draw their weapons to protect the victims sheltering inside.

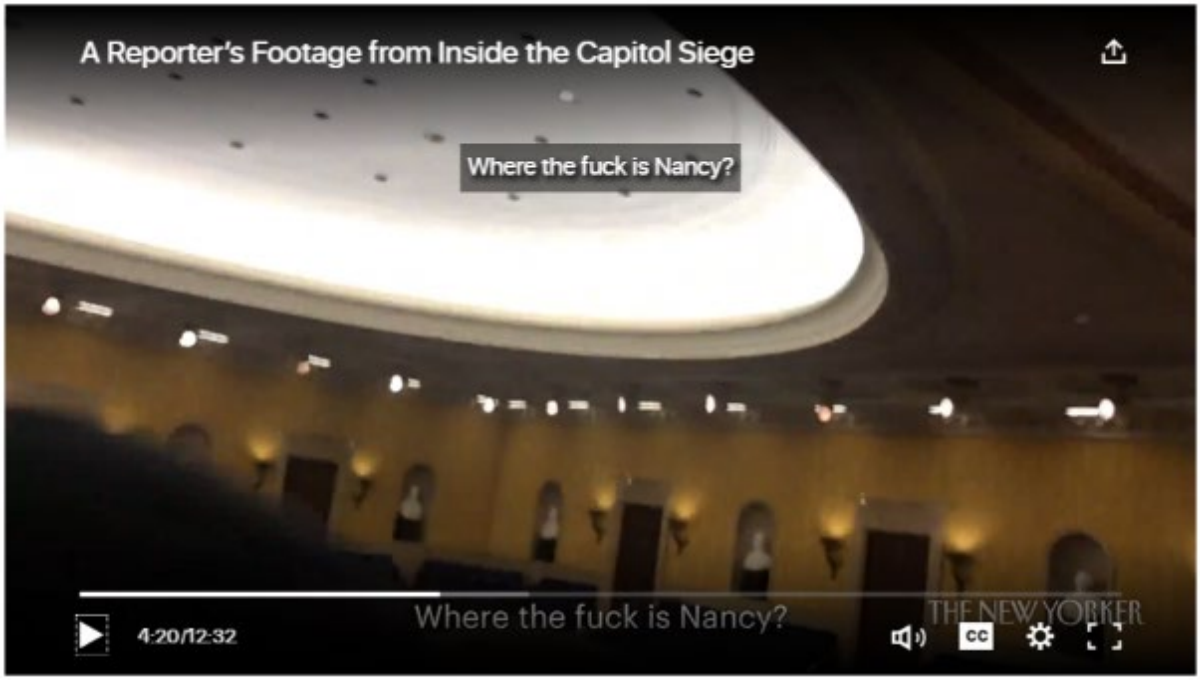
17. At approximately 2:30 p.m., known and unknown subjects broke windows and pushed past USCP and supporting law enforcement officers forcing their way into the U.S. Capitol on both the west side and the east side of the building. Once inside, the subjects broke windows and doors, destroyed property, stole property, and assaulted federal police officers. Many of the federal police officers were injured, several were admitted to the hospital, and at least one federal police officer died as a result of the injuries he sustained. The subjects also confronted and terrorized members of Congress, Congressional staff, and the media. The subjects carried weapons including tire irons, sledgehammers, bear spray, and tasers. They also took police equipment from overrun police including shields and police batons. At least one of the subjects carried a handgun with an extended magazine. These actions by the unknown individuals resulted in the disruption and ultimate delay of the vote Certification.

18. Also at approximately 2:30 p.m., as subjects reached the rear door of the House Chamber, USCP ordered the evacuation of lawmakers, Vice President Mike Pence, and president pro tempore of the Senate, Charles Grassley, for their safety.

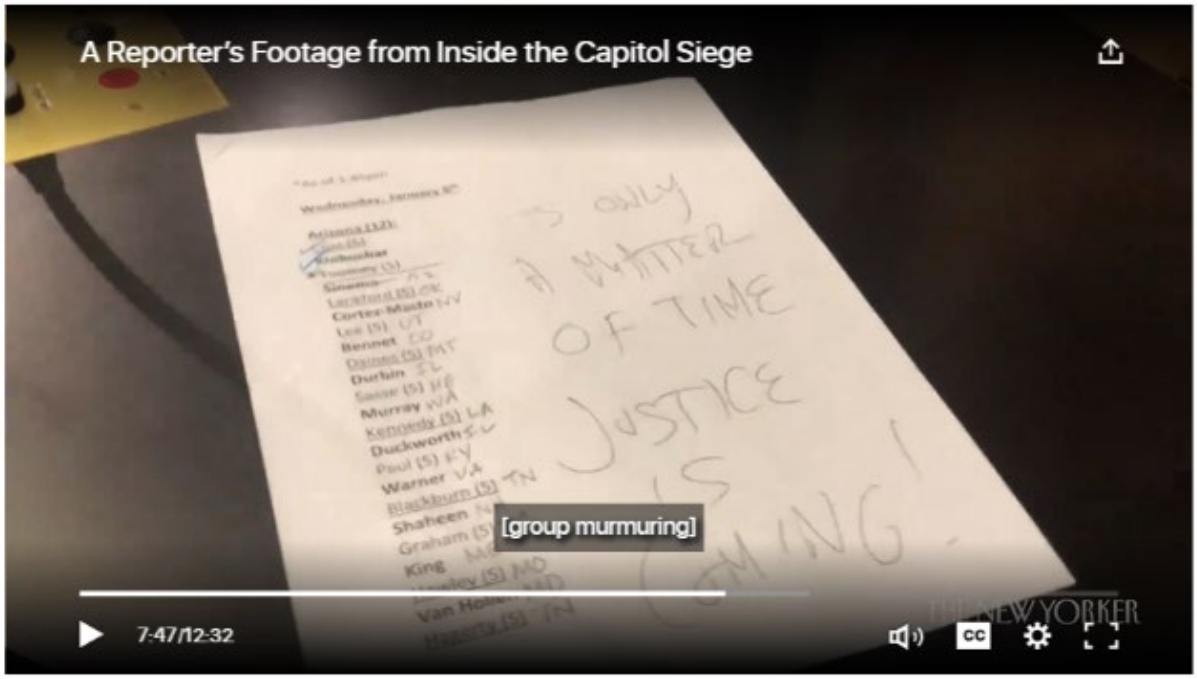
19. At around 2:45 p.m., subjects broke into the office of House Speaker Nancy Pelosi. At about the same time, one subject was shot and killed while attempting to break into the House chamber through the broken windows.

20. At around 2:47 p.m., subjects broke into the United States Senate Chamber. Publicly available video shows an individual asking, "Where are they?" as they opened up the door to the Senate Chamber. Based upon the context, law enforcement believes that the word "they" is in reference to members of Congress.


21. After subjects forced entry into the Senate Chamber, publicly available video shows that an individual asked, "Where the fuck is Nancy?" Based upon other comments and the context, law enforcement believes that the "Nancy" being referenced was the Speaker of the House of Representatives, Nancy Pelosi.




22. A subject left a note on the podium on the floor of the Senate Chamber. This note, captured by the filming reporter, stated "It's Only A Matter of Time Justice is Coming."




23. During the time when the subjects were inside the Capitol building, multiple subjects were observed inside the U.S. Capitol wearing what appears to be, based upon my training and experience, tactical vests and carrying flex cuffs. Based upon my

knowledge, training, and experience, I know that flex cuffs are a manner of restraint that are designed to be carried in situations where a large number of individuals were expected to be taken into custody.

24. At around 2:48 p.m., DC Mayor Muriel Bowser announced a citywide curfew beginning at 6:00 p.m.

25. At about 3:25 p.m., law enforcement officers cleared the Senate floor.

26. Between 3:25 and around 6:30 p.m., law enforcement was able to clear the U.S. Capitol of all of the subjects.

27. Based on these events, all proceedings of the United States Congress, including the joint session, were effectively suspended until shortly after 8:00 p.m. the same day. In light of the dangerous circumstances caused by the unlawful entry to the U.S. Capitol, including the danger posed by individuals who had entered the U.S. Capitol without any security screening or weapons check, Congressional proceedings could not resume until after every unauthorized occupant had left the U.S. Capitol, and the building had been confirmed secured. The proceedings resumed at approximately 8:00 pm after the building had been secured. Vice President Pence remained in the United States Capitol from the time he was evacuated from the Senate Chamber until the session resumed.

28. Beginning around 8:00 p.m., the Senate resumed work on the Certification.

29. Beginning around 9:00 p.m., the House resumed work on the Certification.

30. Both chambers of Congress met and worked on the Certification within the Capitol building until approximately 3:00 a.m. on January 7, 2021.

31. During national news coverage of the aforementioned events, video footage which appeared to be captured on mobile devices of persons present on the scene depicted evidence of violations of local and federal law, including scores of individuals inside the U.S. Capitol building without authority to be there.

32. Based on my training and experience, I know that it is common for individuals to carry and use their cell phones during large gatherings, such as the gathering that occurred in the area of the U.S. Capitol on January 6, 2021. Such phones are typically carried at such gatherings to allow individuals to capture photographs and video footage of the gatherings, to communicate with other individuals about the gatherings, to coordinate with other participants at the gatherings, and to post on social media and digital forums about the gatherings.

33. Many subjects seen on news footage in the area of the U.S. Capitol are using a cell phone in some capacity. It appears some subjects were recording the events occurring in and around the U.S. Capitol and others appear to be taking photos, to include photos and video of themselves after breaking into the U.S. Capitol itself, including photos of themselves damaging and stealing property. As reported in the news media, others inside and immediately outside the U.S. Capitol live-streamed their activities, including those described above as well as statements about these activities.

34. Photos below, available on various publicly available news, social media, and other media show some of the subjects within the U.S. Capitol during the riot. In several of these photos, the individuals who broke into the U.S. Capitol can be seen holding and using cell phones, including to take pictures and/or videos:

[1]

[1] https://losangeles.cbslocal.com/2021/01/06/congresswoman-capitol-building-takeover-an-attempted-coup/

 [2]

 [3]

35. As the proceedings continued in both the House and the Senate, and with Vice President Mike Pence present and presiding over the Senate, a large crowd gathered outside the U.S. Capitol. As noted above, temporary and permanent barricades were in place around the exterior of the U.S. Capitol building, and U.S. Capitol Police

[2] https://www.businessinsider.com/republicans-objecting-to-electoral-votes-in-congress-live-updates-2021-1.

[3]https://www.thv11.com/article/news/arkansas-man-storms-capitol-pelosi/91-41abde60-a390-4a9e-b5f3-d80b0b96141e

were present and attempting to keep the crowd away from the Capitol building and the proceedings underway inside.

36. At such time, the certification proceedings were still underway and the exterior doors and windows of the U.S. Capitol were locked or otherwise secured. Members of the U.S. Capitol Police attempted to maintain order and keep the crowd from entering the Capitol; however, shortly around 2:00 p.m., individuals in the crowd forced entry into the U.S. Capitol, including by breaking windows and by assaulting members of the U.S. Capitol Police, as others in the crowd encouraged and assisted those acts.

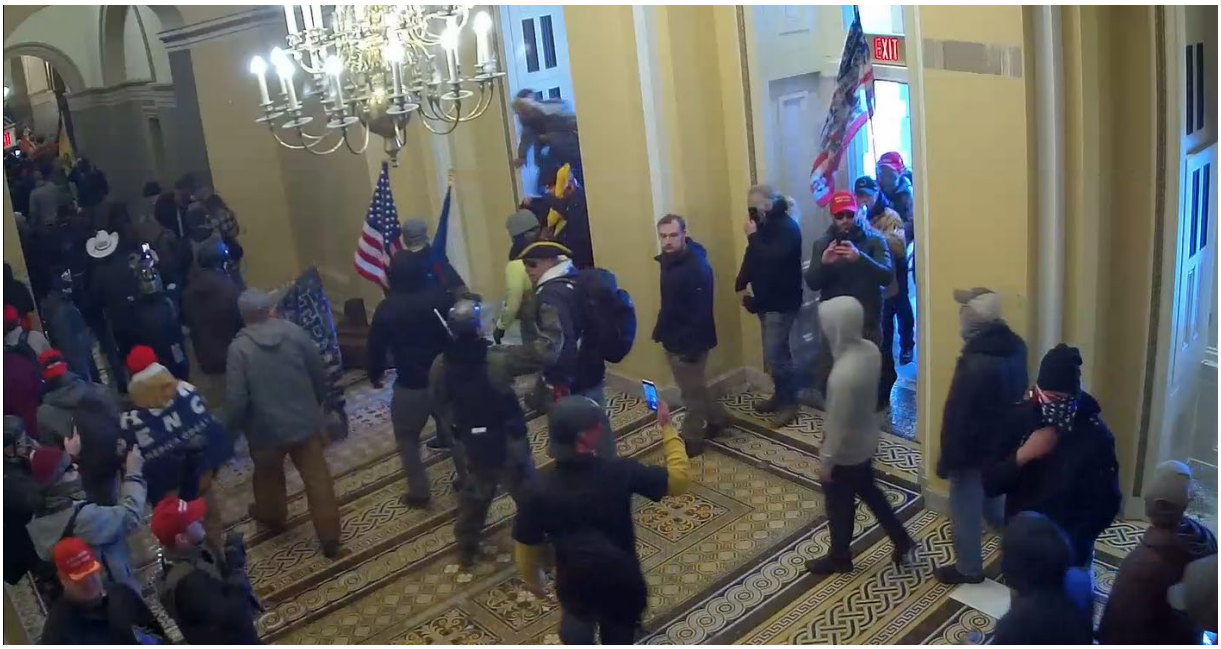
37. Shortly thereafter, at approximately 2:20 p.m. members of the United States House of Representatives and United States Senate, including the President of the Senate, Vice President Mike Pence, were instructed to—and did—evacuate the chambers. Accordingly, the joint session of the United States Congress was effectively suspended until shortly after 8:00 p.m. Vice President Pence remained in the United States Capitol from the time he was evacuated from the Senate Chamber until the sessions resumed.

38. During national news coverage of the aforementioned events, video footage which appeared to be captured on mobile devices of persons present on the scene depicted evidence of violations of local and federal law, including scores of individuals inside the U.S. Capitol building without authority to be there.

### *Facts Specific to This Application*

39. Following this incident, FBI agents reviewed several open source videos in addition to video footage provided by the U.S. Capitol Police depicting the breach of security at the Capitol and several indoor areas where violators were observed.

40. Upon review of the video footage obtained from U.S. Capitol Police, at approximately 14:17:53, a male wearing a dark colored jacket, a black and tan fur-lined hat, and a black shirt with a yellow and red label on the front ("the Subject Male") was observed entering through the window of the Senate Wing entrance to the Capitol. Below is a screen capture taken from the aforementioned video footage.



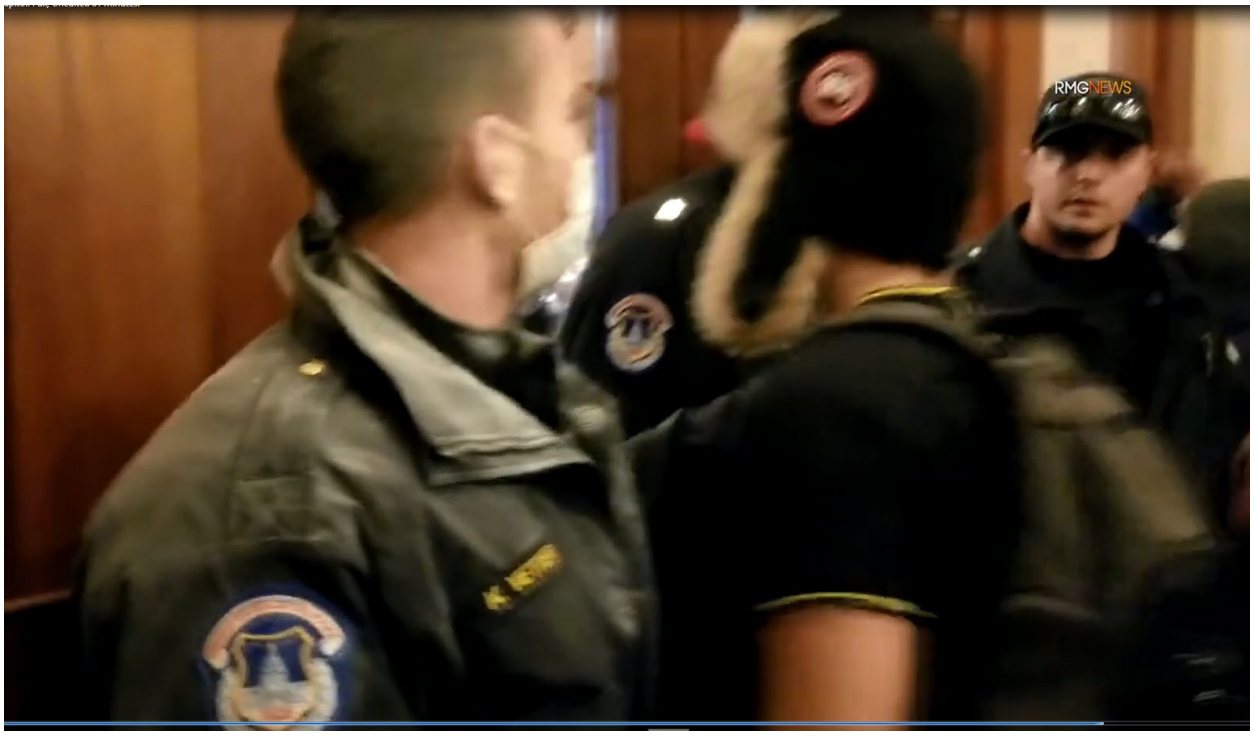

41. The U.S. Capitol Police video footage also shows the Subject Male inside the Main Door Hall at approximately 14:40:24 where he and other violators forced their way past U.S. Capitol Police personnel. The Subject Male was wearing the same black and tan fur-lined hat, dark rimmed glasses, dark pants and the same black shirt with yellow and red logo on the front of it. The logo on the shirt reflects the label "Pirelli" with a "Nike" label on the right-side and an Inter-Milan Soccer Team logo on the left side of it. It is noted, during this time period of the footage, the Subject Male was not wearing the dark colored jacket he was wearing when he first entered the U.S. Capitol. The Subject Male was wearing a gray colored backpack around his shoulders. The Subject Male's demeanor appeared agitated as he walked down the hallway toward the East stairs. The Subject Male then walked toward a U.S. Capitol Police security official wearing a suit and an unknown female. The Subject Male immediately bypassed the female and got close to the U.S. Capitol Police official's face. Below are screenshots captured from the footage showing the Subject Male in these areas within the U.S. Capitol.

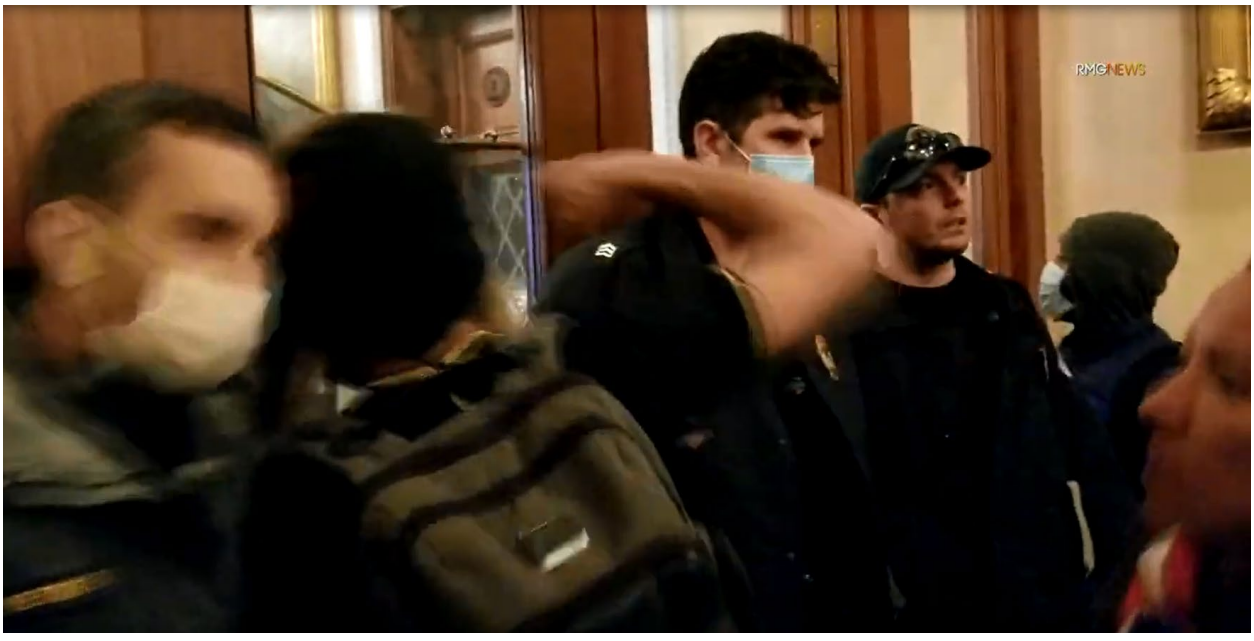
42. Several open source videos were reviewed by FBI agents which also show a large, aggressive crowd, including the Subject Male, trying to breach a barricaded door to the Speaker's Lobby, a hallway that connects to the House of Representatives chambers. The words "Speaker's Lobby" are visible at the top of the doors. Chairs, visible through the door's glass panels, were used to barricade the door from the inside of the Speaker's Lobby. The door was guarded by three Capitol Police officers in front.

43. Videos depicting this entrance to the Speaker's Lobby captured the shooting of a woman identified as Ashli Babbitt. A closer vantage point of the Subject Male showed that the black and tan fur-lined hat had a "Canada Goose" label and that he also wore a red baseball hat underneath the fur-lined hat; he also had dark rimmed glasses and a black mask positioned down on his chin. The Subject Male was observed

repeatedly punching the glass panels of the doors immediately behind the officers, causing the glass to splinter. While throwing two of the punches, the Subject Male pushed his body up against one of the Capitol Police officers guarding the door. Members of the crowd were shouting and gesticulating at the officers. The Subject Male is in video footage shouting "Fuck the blue" multiple times in the faces of the U.S. Capitol Police officers who were standing post outside the Speaker's lobby door. Additional officers in riot gear arrived behind the crowd at the Speaker's Lobby doors, and the three officers guarding the door appeared to move to the adjacent wall.

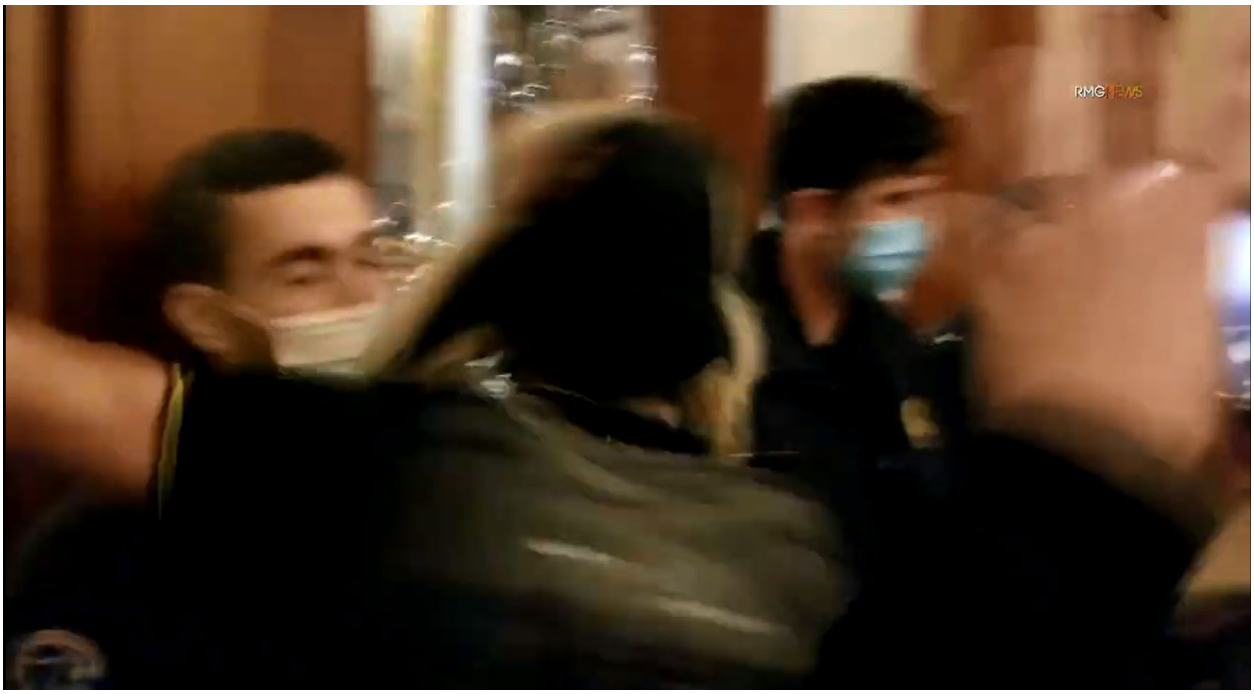
44. Seconds after the officers stepped away from the doorway, the Subject Male began kicking the glass panels of the Speaker's Lobby door. Shortly thereafter, he took a black-colored helmet from an individual with a yellow "Don't tread on me" flag, took off his fur-lined hat and red baseball hat, and violently struck the middle glass panel repeatedly with the helmet, further shattering the window. The Subject Male then smashed the window panel on the right with the helmet. Chants could be heard of "Break it down!" and "Let's fucking go!" Babbitt was shot while attempting to climb through one of the shattered windows. After the shot, the Subject Male backed away toward the stairwell next to the U.S. Capitol Police tactical unit. The Subject Male put the helmet on and wore it as he stood on the steps of the stairwell. Still images from the video are produced below.


RMGNEWS

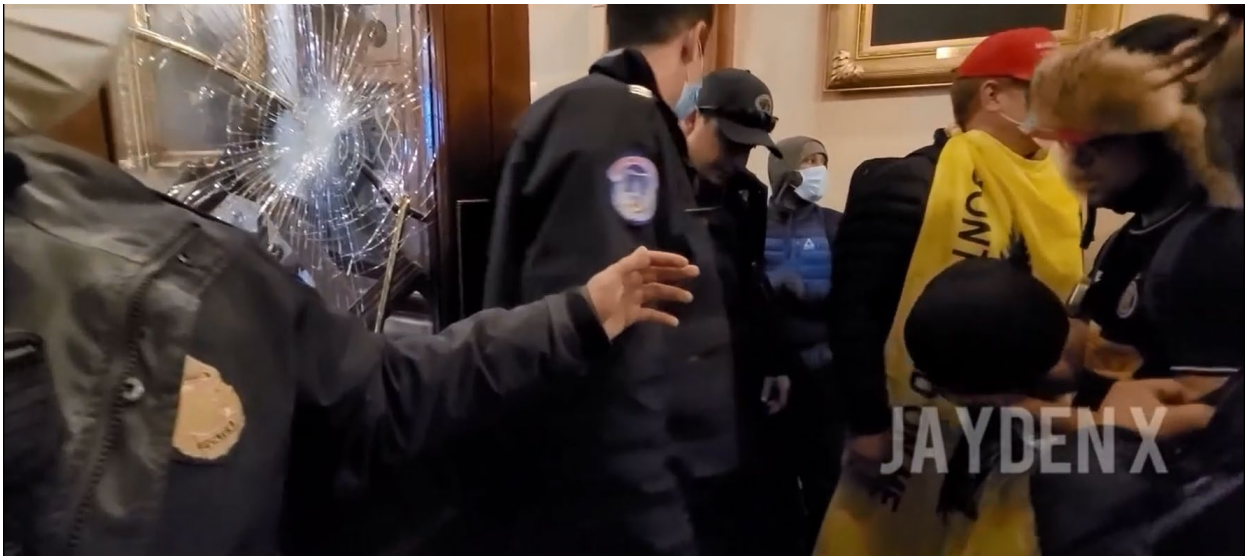

RMGNEWS


RMGNEWS


RMGNEWS


RMG NEWS


JAYDEN X


JAYDEN X


JAYDEN X


JAYDEN X


RMG NEWS

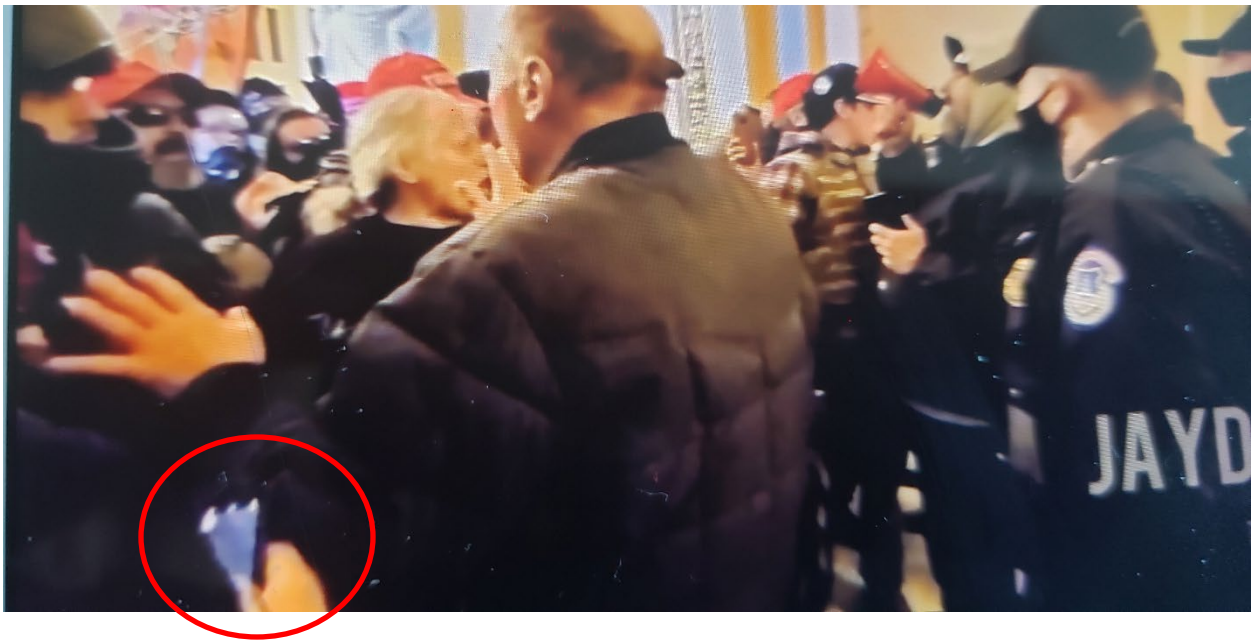

SPEAKERS LOBBY
THERESISTANCE.VIDEO



45. In addition to the distinctive shirt, hat, and helmet that are described above, the video footage also shows the Subject Male wearing a light-colored backpack.


JAYDE


JAYDEN X




46. Additionally, the video footage shows a man matching Alam's description carrying a dark-colored mobile phone, which is circled in the photograph above. Although Alam's face is not shown in the screenshot, review of the video shows that the person holding the phone matches Alam's description.

47. On January 12, 2021, an FBI poster was posted to various social media platforms seeking public assistance in identifying the male. On January 13, 2021, the male was also included on a FBI BOLO which captured his photo as, "BOLO #79."

48. On January 14, 2021, an anonymous tip to the FBI National Threat Operation Center ("NTOC") identified BOLO #79 as the tipster's "Family member," Zachary Alam, providing Alam's age, phone number (718-664-5468), email address, and other identifying information.

49. FBI agents later retrieved a driver's license photo of Zachary Jordan Alam and determined the individual depicted in the driver's license matched the appearance of the Subject Male. FBI agents also viewed a Youtube channel and Facebook profile of Alam based on the name provided by the tip and determined that the photos in the account matched the Subject Male.

50. On January 19, 2021, Witness-1 (hereinafter "W-1") submitted a tip, including his/her contact information, to the FBI NTOC identifying BOLO #79 as his/her relative, Zachary Alam, providing Alam's age, approximate location, and a phone number Alam recently used to call W-1.

51. On January 24, 2021, the FBI interviewed W-1, who provided the following information.

52. W-1 stated that W-1 had submitted the anonymous tip on January 14, 2021, before following up with the tip on January 19.

53. W-1 positively identified Alam, W-1's relative, as the male depicted in BOLO #79. W-1 also was shown several photographs from video footage of the Capitol events described above and identified the Subject Male s Alam, W-1's relative. One of the aforementioned photographs depicts a tattoo "2020" on the Subject Male's inner left arm. W-1 reviewed the photograph with the partial "2020" and advised agents that Alam has such a tattoo and that it states in full, "$250k in 2020." W-1 circled the area and provided his/her initials as confirmation that the Subject Male was Alam.

54. W-1 recognized the black Pirelli shirt bearing the red and yellow logo as Alam's shirt.

55. W-1 stated that a few days after the events at the U.S. Capitol, another relative sent W-1 an open-source video depicting the breaking of the glass windows of the doorway to the Speaker's Lobby. W-1 advised that W-1 and the relative reviewed the video approximately 20 times and confirmed that the male hitting the glass with the helmet was their relative Alam.

56. W-1 told FBI agents about a telephone call she had received from Alam after the January 6, 2021 events. Alam told W-1 that he was sorry for what he had done at the U.S. Capitol but he was not going to turn himself into authorities because he did not want to go to jail again. Alam declined to provide to W-1 his exact location.

57. W-1 also advised that Alam has, since the events at the Capitol, asked relatives if Alam may stay at their residences, and has stated that the FBI is looking for him.

## T-Mobile Toll Records

58. On or about January 22, 2021, FBI agents received subscriber records and toll records for the mobile phone account associated with the telephone number 718-664-5468.

59. According to T-Mobile records, the subscriber information for that account was "Clark Kent," 450 Massachusetts Avenue NW, Washington DC. The records indicated activation since August 23, 2020, and suspension as of January 13, 2021. The phone was shown as a black Apple iPhone 7 with Device ID: 354909097687259; ICCID: 8901260053963175711F. According to W-1, Alam is fixated with Superman. Based on my training and experience, I know that Clark Kent is the name of Superman's alter-ego.

60. According to the call detail records, 718-664-5468 was used to communicate with W-1 over thirty times between December 3, 2020, and January 9, 2021. Additionally, further review of the call detail records showed 718-664-5468 was

used to communicate multiple times with three different close relatives of Alam's and a close associate. As of January 15, 2021, 718-664-5468 communicated via text message with two of Alam's close relatives.

61. On January 26, 2021, FBI agents spoke with a T-Mobile representative Andy LNU regarding the noted suspension date of January 13, 2021. FBI agents were advised that the phone number was still communicating via text message after January 13, 2021. According to Andy LNU, the phone was most likely utilizing Wi-Fi to communicate. Andy LNU further stated that so long as the phone is turned on, the search warrant for the IMEI and/or IMSI would still retrieve necessary geolocation information in order to track the actual phone coordinates.

## Apple Account Records

62. On January 26, 2021, according to account records received from Apple, Inc., DSID account number: 1443500817 is assigned to Zachary Alam, email: zalam91@gmail.com, address: 13726 Cabells Mill Drive, Centreville, VA 20120.

63. According to the records, Alam registered a black IPhone 7 bearing serial number: DX3D243YHG6W to his iCloud on August 23, 2020, which was the activation date shown in the T-Mobile records, described above.

64. Furthermore, according to the iCloud login information, the last known session as of January 21, 2021 was pinging from IP: 172.58.207.75. According to an open source IP geolocation website, this IP address belongs to T-Mobile and was apparently pinging in Dayton, Ohio.

65. Additionally, Apple records show that on or about September 3, 2018, Zachary Alam registered a Macbook Air 13.3/1.6GHZ/8GB/128GB-USA, Part number: MMGF2LL/A, serial: C02T4391H3QD. Based on my training and experience, as well as my review of photographs obtained on the internet of the Macbook Air bearing part number MMGF2LL/A, there is probable cause to believe that the device displays an Apple logo on the top of the computer.

## January 29, 2021 Ping Order

66. On or about January 29, 2021, the Honorable G. Michael Harvey, a United States Magistrate Judge for the District of D.C., issued a "ping" order for telephone number 718-664-5468.

67. Using that ping data, agents tracked Alam to the Subject Premises. Surveillance of the Subject Premises showed an individual matching Alam's description driving a black Chevy pickup truck in and out of the Subject Premises. The pickup truck bore Pennsylvania license plate number KMY7667, which came back to Alam's uncle. Agents observed a second white male in the passenger seat of the pickup truck.

68. W-1 in her first anonymous tip told FBI agents that Alam "drives a black Chevy pickup."

69. During January 29, 2021, surveillance of the Subject Premises, FBI agents observed Alam entering and exiting Room 17.

70. According to an interview of the clerk at the Subject Premises, Alam had reserved his room at the Subject Premises until Wednesday, February 3, 2021.

**January 30, 2021 Arrest**

71. In light of the foregoing, on or about January 25, 2021, Judge Faruqui issued the Arrest Warrant, which FBI agents executed on January 30, 2021 at 8:45 A.M., at the Subject Premises. On that morning, agents knocked and announced their presence and identity. Alam failed to respond. When agents opened the door using a key that had been provided by hotel management, they found Alam hiding behind the entry door. Alam was alone in the room.

72. While effectuating the arrest, the FBI agents observed in plain view items that there is probable cause to believe constitute fruits, evidence and/or instrumentalities of the Subject Offenses.

73. FBI agents observed two mobile phones. One is a dark colored iPhone that matches the physical description of the device observed in the video footage of the January 6, 2021, events, and the device in the Apple records that belongs to Alam. The second mobile phone is a dark-colored flip phone. Based on my training and experience, individuals who are on the run from law enforcement will sometimes acquire a new phone in order to avoid detection by law enforcement. There is probable cause to believe that Alam did so here, and that, before his arrest, he was in possession of two phones.

74. There is probable cause to believe that the two mobile phones contain fruits, instrumentalities, and/or evidence of the Subject Offenses. First, there is probable cause to believe that the cell phones contain attribution evidence, showing that Alam was the owner and user of the phones. Among other things, records of telephone calls, text messages, emails, contact lists, calendars, and photographs can be used to identify the owner and/or user of a mobile phone.

75. Second, there is probable cause to believe that the phones will contain evidence of Alam's location on January 6, 2021, and thereafter. As described above, there is evidence that Alam had in his possession a digital device (namely his cellular phone) while at the U.S. Capitol on January 6, 2021. Based on my training and experience, mobile phones, and especially smart phones like the one observed in the Subject Premises, contain records showing the location of the phone based on GPS and other means. Even non-smart phones may contain location evidence because, based on my training and experience, they may contain evidence of what cell phone towers to which the phone had connected. Additionally, both smart phones and non-smart phones

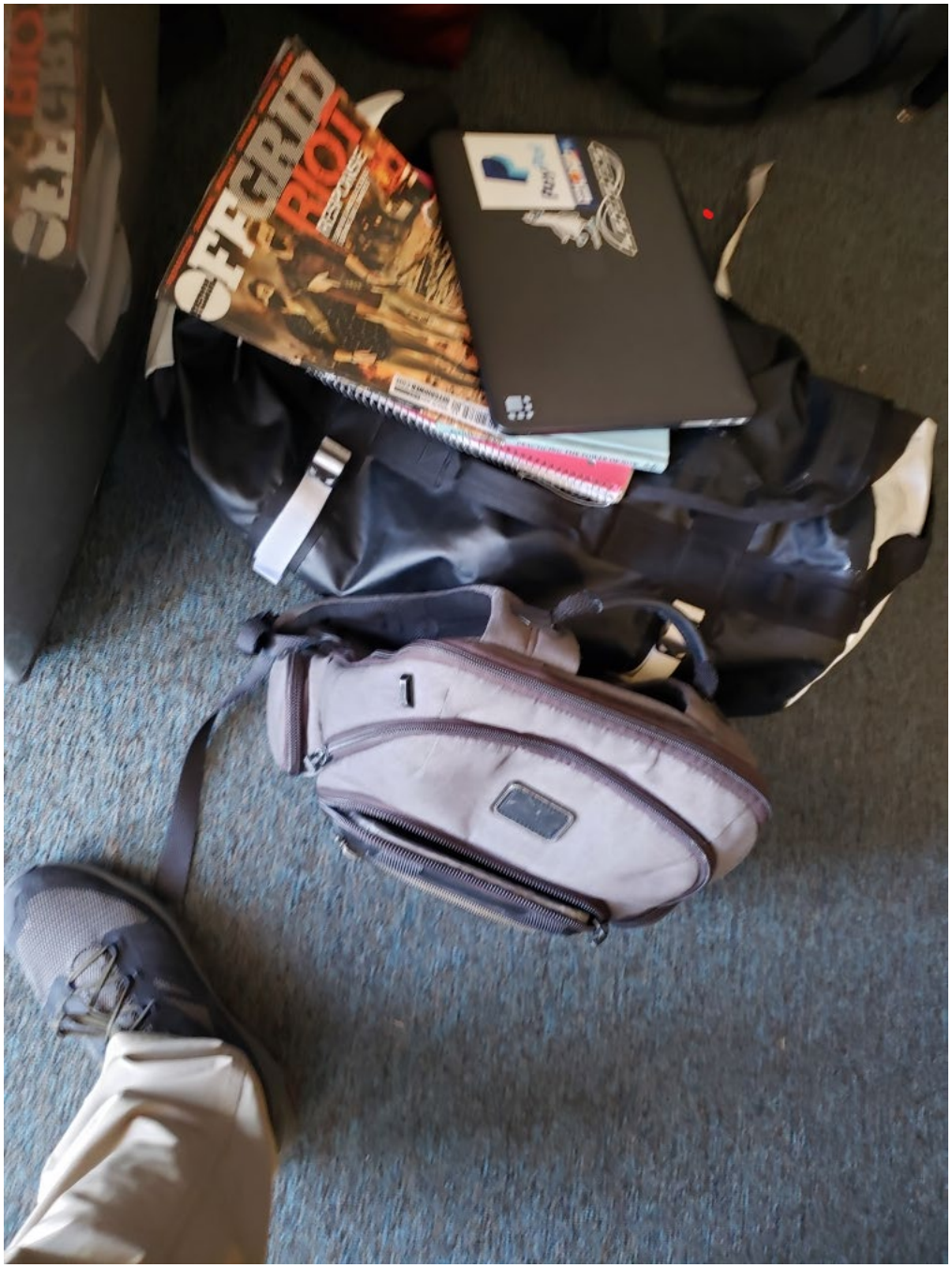
are capable of recording photographs and videos that could show their location at a particular time.

76. Third, based on photos and videos of the offenses that date, numerous persons committing the Subject Offenses possessed digital devices that they used to record and post photos and videos of themselves and others committing those offenses.

77. Fourth, there is probable cause to believe that the cell phones contain communications relating to the Subject Offenses. Based on the investigation, numerous persons committing the Subject Offenses possessed digital devices to communicate with other individuals to plan their attendance at the gatherings, to coordinate with other participants at the gatherings, and to post on social media and digital forums about the gatherings. Evidence of prior communications or communications during the riot coordinating efforts or making plans in the form of text messages, exchanged videos or images, or voicemails are all relevant evidence that would tend to show violations of the Target Offenses.

78. Moreover, location information from Alam's phones, photos and videos taken on January 6, calls made on January 6 and plans made prior to that date, text messages both before and after that date discussing what occurred, are all relevant evidence of the Subject Offenses. Alam's location after January 6, 2021, could confirm that he was on the run from law enforcement.

79. FBI agents also observed a light-colored backpack, pictured below, which matches the description of the backpack that Alam was carrying on January 6, 2021. That backpack links Alam to the events of January 6, 2021.




80. FBI agents also observed a laptop computer, shown in the photograph above, in the Subject Premises. The laptop computer shows a faint Apple logo on the top, which is consistent with the description of the computer that Alam registered to his

Apple account.[4] In my training and experience, it is common for individuals to back up or preserve copies of digital media (such as photos and videos) across multiple devices to prevent loss. Indeed, some companies provide services that seamlessly sync data across devices, such as Apple devices and the Apple iCloud service. Thus, there is reason to believe that evidence of the offense that originally resided on the Subject's cell phone may also be saved to other digital devices within the Subject Premises. Moreover, here, as widely reported in the news media related to this matter, many individuals committing the Target Offenses kept and posted videos, photos, and commentary about their participation in these offenses, essentially bragging about their participation. Based on that, there is also probable cause to believe that evidence related to these offenses may have been transferred to and stored on digital devices beyond the particular digital device the Subject possessed during the offenses.

81. FBI agents also observed the magazine "Recoil OffGrid," which is shown above and which, according to the website associated with the magazine, has an audience of people who are interested in living "off the grid" which means outside of civilization. The title of the lead article in the magazine is "Riot Response, Survive and Succeed During Civil Unrest." There is probable cause to believe that Alam possessed this magazine in preparation for the civil unrest that he participated in on January 6, 2021. There is probable cause to believe that the Subject Premises contains other similar periodicals or training materials relating to civil unrest.

82. The Subject Premises also contains a spiral bound notebook, displayed in the photograph above. Based on my training and experience, and discussions with other law enforcement officers, as well as the investigation in this case and the FBI's investigation in dozens of other cases relating to the intrusion into the U.S. Capitol and the rioting outside of it, I know that individuals like Alam take notes about the research, planning, and implementation of their crimes. There is probable cause to believe that the spiral bound notebook contains fruits, evidence, and/or instrumentalities of the Subject Offenses. There is also probable cause to believe that the Subject Premises contains other such repositories of research, planning and implementation of the Subject Offenses.

83. Based on my training and experience, and discussions with other law enforcement officers, as well as the investigation in this case and the FBI's investigation in dozens of other cases relating to the intrusion into the U.S. Capitol and the rioting outside of it, I know that individuals participating in the Subject Offenses carry their electronic devices on their person and in their vehicles as they travel from place to place. Specifically:

---

[4] There is probable cause to believe that laptop computer is covered with a protective covering of some sort. The ports of the computer, which are visible on the side of the computer, are light colored, while the laptop itself is much darker.

a. Those making plans to travel in internet commerce and/or organizing efforts to riot in the way that Alam and others rioted and/or to assault officers often maintain evidence of their criminal activity at locations that are convenient to them, such as their residences and inside their vehicles. This evidence often includes research related to their plans and other documentary evidence relating to commission of their crimes. Those making such plans sometimes take or cause to be taken photographs and/or video recordings of themselves and their illegal activity and may have photo or video security systems that record images from their homes or property. These individuals usually maintain these photographs and recordings in their possession, at their premises, or at some other safe place.
b. Based on my training and experience, I am aware that persons involved in such activities will typically keep the instrumentalities of their crime, including but not limited to the electronic devices, to include computers, cellular telephones and tablets, used in the commission of the aforementioned offenses in their residences. As described above and in Attachment B, this application seeks permission to search for records that might be found in the Subject Premises, in whatever form they are found. One form in which the records might be found is data stored on electronic devices, computer hard drives, or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

84. Based on my training and experience, and on conversations I have had with other law enforcement officers, I know that some individuals who participate in activities aimed at disrupting or interfering with governmental and/or law enforcement operations have been known to use anonymizing services and/or applications capable of encrypting communications to protect their identity and communications. By using such tools, in some cases, the only way to see the content of these conversations is on the electronic device that had been used to send or receive the communications.

85. The property to be searched includes laptop computers, mobile phones, and/or tablets owned, used, or controlled by Alam, all of which he may have used to communicate about his plans to travel to D.C. on January 6 or about what he did on January 6 while there. Moreover, these devices are likely to contain evidence of Alam's affiliation with other participants and, of other contact he may have had with individuals that were at the riot both prior to and subsequent to the riot, of Alam's motivation to riot, and of planning and organizational efforts. Moreover, these devices may contain evidence of other photographs of Alam wearing the same clothing he wore on January 6, 2021, the use or purchase of the flip phone, and/or records establishing or memorializing his plans.

## TECHNICAL TERMS

86. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. "Digital device," as used herein, includes the following three terms and their respective definitions:

1) A "computer" means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

2) "Digital storage media," as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks ("DVDs"), USB flash drives, flash memory cards, and internal and external hard drives.

3) "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

b. "Wireless telephone" (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through "wi-fi" networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional "land line" telephones, computers, and other digital devices. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic "address

books"; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system ("GPS") locating and tracking technology, and accessing and downloading information from the Internet.

c. A "tablet" is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, "wi-fi" networks, or otherwise. Tablets typically contain programs called applications ("apps"), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

d. A "GPS" navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated "GPS") to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. "Computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. Internet Protocol ("IP") Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic

sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. The "Internet" is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. "Internet Service Providers," or "ISPs," are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line ("DSL"), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

j. A "modem" translates signals for physical transmission to and from the ISP, which then sends and receives the information to and from other computers connected to the Internet.

k. A "router" often serves as a wireless Internet access point for a single or multiple devices, and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. A router usually retains logs for any devices using that router for Internet connectivity. Routers, in turn, are typically connected to a modem.

l. "Domain Name" means the common, easy-to-remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first-level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example,

www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

p. "Encryption" is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

q. "Malware," short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.

## COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS

79. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found on the Subject Premises, in whatever form they are found. One form in which such items might be found is data stored on one or more digital devices. Such devices are defined above and include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus, the warrant applied for would authorize the seizure of digital devices or, potentially, the copying of stored information, all under Rule 41(e)(2)(B). Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that, if digital devices are found on the Subject Premises, there is probable cause to believe that the items described in Attachment B will be stored in the Device(s) for at least the following reasons:

a. Individuals who engage in criminal activity, including the Target Offenses typically interact with others utilizing digital devices, discuss their feelings or plans with others (both coconspirators and likeminded individuals), and may record

videos or take pictures to show their efforts and whether they have accomplished their objectives. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often "back up" or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

b. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

80. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital device(s) were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the Device(s) at issue here because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole.

Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

f. I know that when an individual uses a digital device to conspire with others to commit a crime and/or to organize criminal activity, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense and the identities of those perpetrating it.

## METHODS TO BE USED TO SEARCH DIGITAL DEVICES

81. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. Recovery of "residue" of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not

present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting "keyword" search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format ("PDF"), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as "AES-256 encryption" to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and

documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

82. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the premises.

a. Therefore, in searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

1. Upon securing the Subject Premises, law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any digital devices (that is, the Device(s)), within the scope of this warrant as defined above, deemed capable of containing the information, records, or evidence described in Attachment B and transport these items to an appropriate law enforcement laboratory or similar facility for review. For all the reasons described above, it would not be feasible to conduct a complete, safe, and appropriate search of any such digital devices at the Subject Premises. The digital devices, and/or any digital images thereof created by law enforcement sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

2. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by "opening," reviewing, or reading the images or first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "keyword" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

3. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized digital devices will be specifically chosen to identify the specific items to be seized under this warrant.

## BIOMETRIC ACCESS TO DEVICE(S)

83. This warrant permits law enforcement agents to obtain from the person of Zachary Alam the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s). The grounds for this request are as follows:

84. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

85. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

86. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

87. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

88. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

89. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices, the Device(s), will be found during the search. The passcode or password that would unlock the Device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

90. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

91. Due to the foregoing, if law enforcement personnel encounter any Device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from the aforementioned person(s) the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the Device(s) found at the Subject

Premises; (2) hold the Device(s) found at the Subject Premises in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the Device(s) found at the Subject Premises in front of the face of the aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s) in order to search the contents as authorized by this warrant.

92. The proposed warrant does not authorize law enforcement to require that the aforementioned person(s) state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s). Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

## AUTHORIZATION TO SEARCH AT ANY TIME OF THE DAY OR NIGHT

93. Law enforcement personnel will commence the execution of this search and seizure warrant upon the Subject Premises during daytime hours (between 6:00 a.m. and 10:00 p.m.), as early as practicable. It is anticipated that law enforcement personnel will attempt to image or copy digital information from certain servers on the Subject Premises, rather than remove those servers from the premises. Such onsite imaging or copying will minimize disruptions to the use of those servers.

94. From my training and experience, I know that imaging or copying information from servers on the Subject Premises can be substantially delayed by various factors which cannot be ascertained or sometimes even anticipated until the actual execution of the warrant. There may, for example, be no system administrator available, willing, or able to assist law enforcement personnel to narrow the search by identifying the virtual or dedicated server(s) on the Subject Premises, or the server folders, containing information within the scope of the warrant. There may be terabytes or even petabytes of information to be copied. The network architecture of the servers on the Subject Premises or the configuration of the server hardware may affect and delay data transfer speeds. Data encryption and password protections may also significantly delay imaging or copying as law enforcement personnel seek to identify necessary passwords without which imaging or copying on the Subject Premises would likely be unachievable. Under some circumstances, data downloads can be interrupted by network or hardware malfunctions or other network or hardware attributes which often necessitates restarting the data downloads from the beginning.

95. For all of the foregoing reasons, I respectfully submit that good cause exists, pursuant to Fed. R. Crim. P. 41(e)(2)(A)(ii), for authorization to execute the search warrant at any time of the day or night. Law enforcement personnel will commence executing the warrant a soon after its issuance as possible. However, given the myriad factors that that may prevent completion of the search and seizure by 10:00 p.m., including those described above, I request authorization to continue the warrant execution past 10:00 p.m., if necessary, until completion of the warrant execution. Suspending the execution at 10:00 p.m. until 6:00 a.m. could compromise data downloads in progress, render stored data subject to alteration or deletion, require securing the Subject Premises during the intervening hours, and prolong the disruption of access to, and use of, the Subject Premises and the digital devices being searched. Additionally, the Subject Premises is empty, and Alam is in the temporary custody of the Federal Detention Center.

## CONCLUSION

96. I submit that this affidavit supports probable cause for a warrant to search the Subject Premises described in Attachment A and to seize the items described in Attachment B.

Respectfully submitted,

/s Eric R. Patterson
**Eric R. Patterson**
**Special Agent**
**Federal Bureau of Investigation**

Subscribed and sworn to before me on **January 30, 2021**

/s/ Lynne A. Sitarski
HONORABLE LYNNE A. SITARSKI
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

***Information Subject to Warrant***

The property to be searched is Room 17 of the Penn Amish Motel, located at 2840 North Reading Road, Denver, PA 17517(the "SUBJECT PREMISES"), further described as a motel room with a red brick façade and white doors. Room 17 has a white door bearing the number 17. On the left side of the door is a window, and on the right side of the door is a fire extinguisher mounted to the wall. Next to the door is a red wooden bench.

## ATTACHMENT B

### *Particular Things to be Seized*

1) The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of 18 U.S.C. § § 111(a) and (b) (interference with official duties); § 1361 (depredation of United States property); § 1512(c)(2) (obstruction of Congress); § 231 (civil disorders); § 1752(a)(1) and (2) (unlawful entry on restricted buildings or grounds); and Title 40 U.S.C. Section 5104(e)(2) (violent entry, disorderly conduct, and other offenses on capitol grounds) (the "Target Offenses") that have been committed by Zachary Alam ("the Subject") as described in the search warrant affidavit; including, but not limited to the following:

   a) Items of clothing or objects that could associate Alam with the events of January 6, 2021, including but not limited to: (i) a yellow and black shirt bearing the word "Pirelli;" (ii) a fur lined hat; (iii) a dark-colored helmet; (iv) a dark-colored jacket; (v) a pair of dark-colored glasses; (vi) a dark-colored face mask; (vii) a light-colored backpack; (viii) dark pants; and (ix) a dark-colored smart phone.

   b) Any mobile phones, including but not limited to the dark-colored smartphone and the dark-colored flip phone.

   c) Any laptop computer, including but not limited to the dark-colored Apple computer.

   d) Evidence concerning planning to unlawfully enter the U.S. Capitol, including any maps or diagrams of the building or its internal offices;

   e) Evidence concerning unlawful entry into the U.S. Capitol, including any property of the U.S. Capitol;

   f) Evidence concerning awareness of the official proceeding that was to take place at Congress on January 6, 2021, i.e., the certification process of the 2020 Presidential Election;

   g) Evidence concerning efforts to disrupt the official proceeding that was to take place at Congress on January 6, 2021, i.e., the certification process of the 2020 Presidential Election;

   h) Evidence concerning the breach and unlawful entry of the United States Capitol, and any conspiracy or plan to do so, on January 6, 2021;

   i) Evidence concerning the riot and/or civil disorder at the United States Capitol on January 6, 2021;

   j) Evidence concerning the assaults of federal officers/agents and efforts to impede such federal officers/agents in the performance of their duties the United States Capitol on January 6, 2021;

k) Evidence of any conspiracy, planning, or preparation to commit those offenses;

l) Evidence concerning efforts after the fact to conceal evidence of those offenses, or to flee prosecution for the same;

m) Evidence of the state of mind of the subject and/or other co-conspirators, *e.g.*, intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation; and

n) Evidence concerning the identity of persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with the unlawful actors about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts.